

Teresa M. Corbin (SBN 132360)
 Christopher Kelley (SBN 166608)
 Thomas C. Mavrakakis (SBN 177927)
 Erik K. Moller (SBN 147674)
 HOWREY SIMON ARNOLD & WHITE, LLP
 301 Ravenswood Avenue
 Menlo Park, California 94025
 Telephone: (650) 463-8100
 Facsimile: (650) 463-8400

Attorneys for Plaintiff SYNOPSYS, INC.

UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO DIVISION

11	SYNOPSYS, INC.,) Case No. CO3-02289 MJJ
12	Plaintiff,)
13	vs.) DECLARATION OF VAN Q. NGUYEN IN
14	RICOH COMPANY, LTD.,) SUPPORT OF SYNOPSYS' OPPOSITION
15	Defendant.) TO RICOH'S MOTION FOR ENTRY OF
16) PROTECTIVE ORDER AND CROSS-
17) MOTION FOR ADOPTION OF SYNOPSYS'
) PROTECTIVE ORDER AND DISCOVERY
) PROCEDURES
)
) Date: February 10, 2004
) Time: 9:30 a.m.
) Ctrm: 11

I, Van Q. Nguyen, hereby declare as follows:

1. I currently serve as Director of IT Security at Synopsys, Inc. ("Synopsys"), a position I have held since October 14, 2002. I joined Synopsys in October 14, 2002. Prior to that I held positions I worked as director of IT security at APL for about two and half years, at Fidelity Investments for two years and at Nokia for five years, all in the area of IT and corporate security. The matters set forth in this declaration are based upon my personal knowledge, except where otherwise indicated, and if called as a witness, I could and would testify competently thereto.

2. As Director of IT Security, I manage the security group within Synopsys' Information Technology department, which employs a total of five persons (myself included), all of whom are computer security professionals and dedicated to security-issues at Synopsys. Additionally, all of the IT department, which includes approximately 168 employees and contractors, help support security

1 functions. Synopsys spends approximately 20% of its annual IT budget on IT security. One of my
2 most important responsibilities as Director of IT Security is to ensure that only authorized persons can
3 have access to Synopsys source code and other highly confidential engineering information stored on
4 Synopsys' servers. To achieve this, Synopsys has established a policy and standards to provide for the
5 comprehensive protection for all Synopsys private and proprietary information assets. These policies
6 and standards are designed to ensure that electronic access to Synopsys' proprietary information,
7 including its source code, are tightly controlled. The security of Synopsys' source code rests on the
8 fact that the code resides only in the closed network of Synopsys' computers, and that only authorized
9 users are able to access this computer network. The source code for Synopsys' logic synthesis products
10 is managed using the ClearCase® software asset management tool. This tool, and the source code that
11 it manages, reside on Synopsys' internal computer network. Users obtain access to the source code
12 through the ClearCase® tool. In order, therefore, to review or edit the code, authorized users connect
13 through the Synopsys computer network to the ClearCase® server, which then provides them with
14 access to the code sections that they need.

15 3. Synopsys ensures the security of its source code by imposing tight restrictions on who
16 may access the source code and by deploying a multi-layer security approach that ensures that only
17 authorized individuals are able to access the ClearCase® server that provides access to the source
18 code. That multi-layer security approach includes (a) network perimeter protection measures, (b)
19 internal network segmentation and security measures, (c) per-system authentication, and a (d)
20 specialized remote access environment. With respect to (a), we have established a firewall controlling
21 all access from outside the Synopsys IT environment to the inside of the environment that includes
22 three layers of antivirus protection, and intrusion detection systems. These measures limit the ability of
23 outsiders without physical access to our network environment to damage and/or access our facilities.
24 With respect to (b), the IT environment is segmented to control inter-facility access. This means that
25 in order to access servers at one Synopsys facility from another facility, a user is required to provide a
26 password that authenticates them as someone with authority to access one segment of the Synopsys
27 network from another. Some portions of the Synopsys network are actually physically isolated from
28 the remainder so that it is impossible to use them to access other portions of the network. Portions of

1 the network used by customers and for teaching purposes are isolated in this manner. With respect to
2 (c), each computer on our network requires password-based logon access. In addition, all portable
3 computers have been individually equipped with a personal firewall and additional antivirus software.
4 Once a user has been authenticated as someone authorized to use a given computer, access to sensitive
5 data and systems, such as the ClearCase® source code repository, requires additional, separate
6 authentication, by way of a separate password identifying the user as someone authorized to access this
7 sensitive data.

8 4. In addition to the network security provisions described above, Synopsys' computer
9 network is further secured by the fact that physical access to each of Synopsys' engineering facilities is
10 strictly controlled. Employees or contractors entering any Synopsys facility are required to display a
11 badge or prove their authority to enter by use of a coded card and PIN. Once within the physical
12 confines of a Synopsys facility, even if users have access to a computer located within that facility,
13 they cannot access Synopsys' engineering materials on the computer network until they provide a
14 password that authenticates them as someone who is entitled to have access to those materials.

15 5. Synopsys also allows a limited number of personnel to access the Synopsys engineering
16 computer network remotely using a virtual private network (VPN) set up across remote dial-in
17 telephone lines and/or across the internet between the physically secured Synopsys computer network
18 and an authorized user's remote computer. The specialized remote access environment referred to
19 above as element (d) of the Synopsys security plan ensures that this remote access is secure. Synopsys
20 uses a VPN client software constructed by Synopsys' IT security group exclusively for use with our
21 VPN. All communications through the VPN are secured by means of industrial grade (128 bit or
22 greater) encryption of all data passed between the secured Synopsys network and the remote computer.

23 6. In order to access the Synopsys network remotely, a Synopsys employee or agent must
24 submit an application. If the application is approved by network administrators, the employee or agent
25 is given a SecurID® token manufactured by RSA Security, Inc. This token is a piece of circuitry,
26 contained within either a key fob housing or a credit-card sized package, that generates and displays a
27 new access code every 60 seconds. The user combines a PIN that is personal to them with the code
28 displayed on the SecurID® token. This allows the system to authenticate that the person requesting

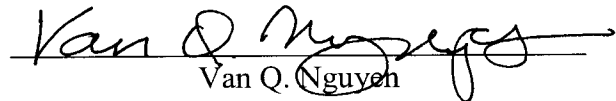
1 access is in possession, in real-time, of the SecurID® token issued to an authorized user and that this
2 person knows a PIN that identifies them as the authorized user to whom the SecurID® token was
3 issued. Once a user has accessed the network using their SecurID® token and PIN, they still must
4 provide additional authentication to access more highly sensitive portions of the network, such as the
5 ClearCase software asset management tool.

6 7. In order to ensure the continuing robustness of the security measures taken by my IT
7 security department, we regularly use vulnerability analysis assessment tools to provide us with
8 advanced notice of any potential defects in network security. In addition, we hire outside vendors to
9 perform penetration analyses and to give us independent assessments of the effectiveness of our
10 security measures.

11 8. Someone from my IT security staff is on call around the clock to ensure that we can
12 respond promptly to any potential security issues that may arise. Our network includes elements that
13 are designed to detect unusual activity and will page or otherwise alert personnel from my team to the
14 existence of any potential developing security breach. We maintain a close working relationship with
15 the persons responsible for security of Synopsys' physical plant so that we can make joint response to
16 any potential threat. In addition, we conduct security awareness training for our employees and
17 operate an intranet site on Synopsys' network dedicated to IT security issues.

18 9. To my knowledge, our efforts to secure access to Synopsys' engineering materials have
19 been successful to date. I am not aware of any instance where unauthorized copies of Synopsys
20 engineering source code were withdrawn from the secured Synopsys computer network.

21 I declare under penalty of perjury under the laws of the United States of America that the
22 foregoing is true and correct. This declaration was executed in Mountain View, California on January
23 20, 2004.

24 
25 Van Q. Nguyen
26
27
28